UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
An Apple Laptop Computer, Model #A1708, Serial #FVFVX2K8Hv22, Currently Located at the Homeland Security Investigations Offices, 401 S. Salina Street, Suite 208, Syracuse, NY, further described in Attachment A

Case No. 5:18-mj-319 (DEP)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
An Apple Laptop Computer, Model #A1708, Serial #FVFVX2K8Hv22, Currently Located at the Homeland Security Investigations Offices, 401 S. Salina Street, Suite 208, Syracuse, NY, further described in Attachment A

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 1546, 1543, 1544, 1028, 1028A, 1030, 1343, 1344, 1349 & 1956(h)	Visa Fraud, Passport Fraud, Misuse of Passport, Identity Theft, Aggravated Identity Theft, Computer Fraud, Wire Fraud, Bank Fraud, Conspiracy to Commit Wire and Bank Fraud, and Conspiracy to Launder Monetary Instruments

The application is based on these facts:
See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jason E. Fulton
Applicant's signature

Jason E. Fulton, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/11/2018

David E. Peebles
Judge's signature

City and state: Syracuse, New York

Hon. David E. Peebles, United States Magistrate Judge
Printed name and title

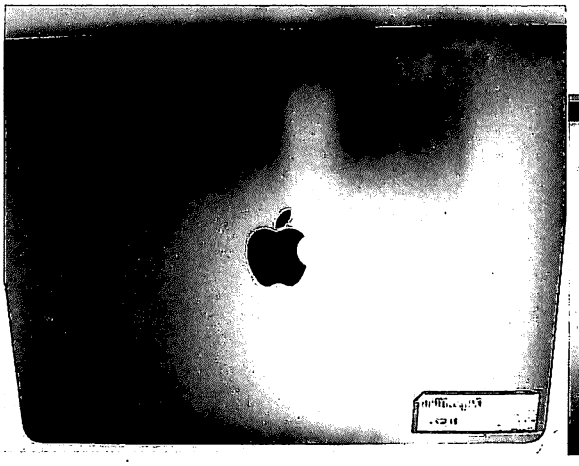
ATTACHMENT A

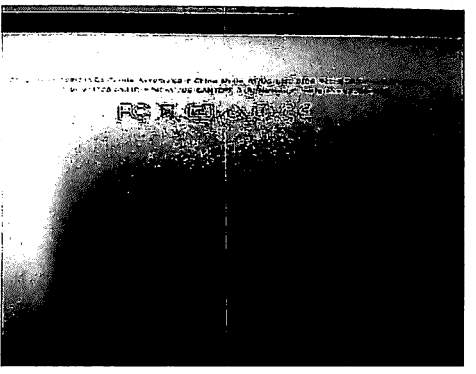
Property to Be Searched

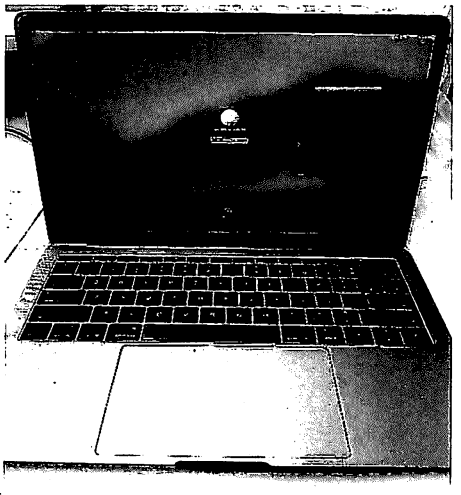
The property to be searched is an Apple Mac Laptop Computer, Model Number: A1708, that is silver in color. The computer is labeled with the serial number: FVFVX2K8Hv22 and FCC ID: BCGA1708.

The Computer currently is located at the Homeland Security Investigations Offices in Syracuse, New York. This Warrant authorizes the forensic examination of the computer for the purpose of identifying the electronically stored information described in Attachment B.

Photographs of the computer to be searched are as follows:







ATTACHMENT B

ITEMS TO BE SEIZED

1. All records on the SUBJECT COMPUTER described in Attachment A that relate to the fruits, instrumentalities and evidence of violations of Title 18, United States Code, Sections 1546 (Visa Fraud),1543 (Passport Fraud), 1544 (Misuse of Passport), 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1030 (Computer Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire and Bank Fraud), and 1956(h) (Conspiracy to Launder Monetary Instruments), and involve OFORI and OFORI's co-conspirators, to include:

a. All documents, communications or other information related to the gathering, purchase, theft, sale or use of identities and personal identifying information, including records of Internet activity, such as Internet Protocol ("IP") addresses, browser history, caches, cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

b. All documents, communications or other information related to the use of anonymizer software, including but not limited to The Onion Router ("TOR") browser.

c. All documents, communications or other information related to the transferring or attempted transferring of money by wire, between bank accounts and/or by or between credit card processing accounts, or other means, including the nature, source, destination, and use of those funds.

d. All documents, communications or other information related to the purchase, creation, transmission, or use of stolen, falsified, fraudulent, or fake credit cards, debit cards, gift cards, or other access devices.

e. All documents, communications or other information related to the obtaining, using, selling, or transmitting of stolen, fake, fraudulent, or falsified personal identifying information or financial information, including but not limited to names, Social Security numbers, dates of birth, addresses, credit card numbers, and bank accounts.

f. All documents, communications or other information related to the structuring or other concealment of transfers and/or withdrawals.

g. All documents, communications or other information regarding the usernames, phone numbers, emails, Skype or instant messenger names used by the co-conspirators and/or their associates to transmit information, including personally identifiable information, credit card numbers, and false identification documents used in the schemes.

h. All documents, communications, or other information related to victims of business email compromises, computer intrusions, romance fraud, and related schemes and artifices to defraud victims of money and property that relate to OFORI and his co-conspirators.

i. All documents, communications or other information related to OFORI's or his co-conspirators travel.

j. All business records, bank records, documents and communications related to entities involving OFORI and OFORI's co-conspirators, including: Edgar Financial Services, LLC; Ellis Global Services, LLC; Lois Global Associates, LLC; Freeman Auto, LLC; Unilever Global, LLC; Pascal Consultancy, LLC; Sackey Settlement Group; Hags Logistics; Prince Fos Investments; and Prince of Peace Cleaning.

k. All documents relating to the immigration status, passports, visas and other travel documents associated with OFORI and his co-conspirators.

1. All employment records, employment applications, earnings information, State and Federal tax returns and tax information, and residential information related to OFORI and his co-conspirators.

2. Evidence of user attribution showing who used or owned the at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "documents" "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF AN APPLE LAPTOP COMPUTER, Model Number A1708, serial number FVFVX2K8Hv22, CURRENTLY LOCATED AT THE HOMELAND SECURITY INVESTIGATIONS OFFICES 401 S. Salina St. Suite 208 Syracuse, NY 13202	No. **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, Jason E. Fulton, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations (HSI) within United States Immigration and Customs Enforcement("ICE") assigned to the Special Agent in Charge, District of Columbia Office in Fairfax, VA. I have been a Special Agent for ICE/HSI and a predecessor the United States Customs Service since October 2001. My duties as a Special Agent include investigating violations of U.S. Immigration and Customs laws. I successfully completed the Criminal Investigator Training Program, Customs Basic Enforcement School, the Identity and Benefit Fraud Training Program Agent Training Program and Worksite Enforcement Program at the Federal Law Enforcement Training Center in Glynn County, Georgia. I have successfully completed the ICE Forensic Laboratory (FL), Document Instructor Training Course in McLean, VA.

2. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a Search Warrant authorizing the search of an Apple Mac Laptop Computer, Model Number A1708, serial number FVFVX2K8Hv22, silver in color

("SUBJECT COMPUTER"),which was lawfully seized at the U.S.-Canada border, and taken by U.S. Customs and Border Protection ("CBP") incident to the administrative arrest of Jeremy Edgar OFORI YENTUMI (hereinafter, "OFORI"), on or about May 27, 2018. CBP Officers detained OFORI at Alexandria Bay, New York, in the Northern District of New York, when he presented a fraudulently-obtained genuine U.S. passport under the name of another person, identified here as E.H. The passport bore the picture of OFORI. OFORI has been subject to an Immigration Judge's order of removal since 2009. He has been in the United States illegally for many years and has engaged in a number of crimes, described further below.

3. The facts described below were acquired as a result of a joint investigation by Special Agents of Homeland Security Investigations ("HSI"), Social Security Administration ("SSA"), and the United States Postal Inspection Service ("USPIS"). Moreover, I have learned additional relevant information from the Federal Bureau of Investigation ("FBI") concerning OFORI and his co-conspirators. The facts recited below are based on my personal knowledge of this investigation and the observations of other law enforcement officials, including a review of documents related to this investigation, witness interviews, and communications with others who have personal knowledge of the events and circumstances described herein. This affidavit is intended to merely show that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

OVERVIEW AND SUMMARY OF VIOLATIONS

4. OFORI is a national of Ghana and not a United States citizen. After a period of time residing in the country with status,[1] OFORI failed to appear before an Immigration Judge

[1] Around May 22, 2004, OFORI was admitted into the United States of America at John F. Kennedy International Airport ("JFK") as a nonimmigrant visitor. On or about January 28, 2005, OFORI was admitted again at JFK as a nonimmigrant visitor, authorized to stay until July

and, subsequently, the Immigration Judge ordered him removed on or about February 23, 2009. Despite this order of removal, OFORI, through the use of fraudulent documents, has managed for years to reside and illegally work in the United States, specifically in the Eastern District of Virginia. Recently, OFORI has become involved in fraud schemes and money laundering as he has received and attempted to receive multiple large wire transfers to accounts he controls through limited liability corporations, using his own identity and the identities of others. The wire transfers appear to be the proceeds of Romance Fraud and Business E-mail Compromises ("BECs"), defined further below, conducted by co-conspirators known and unknown to me.

5. In sum, based on my training and experience and the facts set forth below, I submit that there is probable cause to believe that OFORI and his co-conspirators have engaged in violations of Title 18, United States Code, Sections 1546 (Visa Fraud),1543 (Passport Fraud), 1544 (Misuse of Passport), 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1030 (Computer Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire and Bank Fraud), and 1956(h) (Conspiracy to Launder Monetary Instruments), and that evidence, fruits and instrumentalities of these crimes exist on the SUBJECT COMPUTER.

VISA FRAUD and PASSPORT FRAUD SCHEME

6. In early 2018, OFORI came to my attention due to official inquiries from local law enforcement. I learned that an Immigration Judge had ordered OFORI removed from the United States on or about February 23, 2009. Despite that order, I learned that OFORI has been

---

27, 2005. In violation of his admission, OFORI stayed beyond July 27, 2005. On or about November 7, 2005, OFORI filed a DHS Form I-485, Application to Register Permanent Residence or to Adjust Status, which was denied on or about May 14, 2007. On or about July 27, 2007, OFORI again filed a DHS Form I-485, Application to Register Permanent Residence of Adjust Status, which was denied on or about December 8, 2008. OFORI filed the DHS Form I-485's based on his marriage to a United States citizen. If approved, OFORI would have been allowed to remain in the United States as a Lawful Permanent Resident. Following the denial of his last DHS Form I-485, OFORI was issued a Notice to Appear before an Immigration Judge.

a certified security guard in Virginia. I verified the security guard certification by checking the Virginia Department of Criminal Justice Services public online database. Based on this determination, I suspected that OFORI unlawfully obtained employment. I determined that OFORI obtained employment with at least two different employers, specifically as a security guard with Eagle Protection Services in Manassas, Virginia, and as a counselor with the Prince William County Government. Therefore, using subpoenas, I obtained documents from OFORI's employers. These documents include a DHS Form I-9 (Employment Eligibility Verification), copies of identification documents, employment emergency contact information and an application of employment from each employer.

7. After review of the DHS Form I-9 from Eagle Protection Services, I determined that OFORI falsely claimed to be a lawful permanent resident. OFORI used a Maryland Driver's License and a Social Security Card to fulfil the document requirements for completion of the DHS Form I-9 for Eagle Protection Services. The DHS Form I-9 appears to have been signed and dated by OFORI on October 30, 2015.

8. Based on records checks, I determined that OFORI was last authorized to engage in employment in the United States for the period March 31, 2008 through March 30, 2009. Employment authorization was granted by U. S. Citizenship and Immigration Services while OFORI's applications to adjust status was pending. Employment authorization allows aliens to lawfully obtain Social Security cards and numbers, which OFORI appears to have done. However, following the denial of OFORI's last application to adjust status to a lawful permanent resident, his case was referred to an Immigration Judge, who ordered him removed on or about

February 23, 2009 after he failed to appear before the Immigration Court. That order effectively terminated his right to be in the United States and his employment authorization.[2]

9. The social security card that OFORI presented along with the DHS Form I-9 appears to have been forged or altered. Although OFORI's true name and Social Security number appear on the card, the font on the card appears to be incorrect and the card is missing the required warning, "VALID FOR WORK ONLY WITH DHS AUTHORIZTION." This warning invariably would have been placed on OFORI'S officially issued card based on his immigration status when the original and true social security card and number were issued in or around January 2006. I believe that OFORI produced or caused the production of a Social Security Card with his correct information but with the employment warning omitted.

10. On or about March 12, 2018, I obtained OFORI'S employment documentation from Prince William County. These documents include a DHS Form I-9, E-Verify documentation, a tax withholding form, copies of identification documents, employment emergency contact information and an application for employment. Upon review of the DHS Form I-9, it appears that OFORI falsely claimed to be a United States citizen. OFORI used a Maryland Driver's License and a Social Security Card to fulfil the document requirements for completion of the DHS Form I-9. The Social Security Card again did not have the warning, "VALID FOR WORK ONLY WITH DHS AUTHORIZTION." This DHS Form I-9 appears to have been signed and dated by OFORI on May 9, 2016.

11. Per the guidance on the DHS Form I-9, employers may accept a Social Security card and another document such as a driver's license only if the Social Security card does not

[2] Typically, the Employment Authorization is cancelled upon denial of the I-485, and the applicant is mailed notification. In any event, OFORI's last authorization to work ended at the denial of the I-485, or on the expiration date of the Employment Authorization Document.

have the "VALID FOR WORK ONLY WITH DHS AUTHORIZTION" warning on the card. If the Social Security Card has this warning, the employer is required to ask the employee to produce another document to establish a legal basis to engage in employment in the United States. Examples of these documents include a Lawful Permanent Resident card, Employment Authorization Document or U.S. passport. I believed that OFORI used an altered Social Security card with the employment warning omitted in order to avoid having to produce these other documents, which are more difficult to alter and/or forge.

12. With cooperation from local law enforcement, I was able to determine that on or about June 10, 2016, OFORI fraudulently applied for and ultimately obtained a genuine Virginia Driver's License issued in the name of E. H., but with the picture of OFORI. Also, OFORI apparently attempted to title a vehicle in both his own true name and in the name of E.H.

13. On or about March 23, 2018, I conducted a search of United States passport records and found a passport application for E. H. The picture on the application appears to match OFORI'S immigration and driver's license photographs. It should be noted that the application was not initially accepted because the birth certificate for E.H. did not have a parent's name listed on it. Yet, the passport application had listed both parents, including the name Faustina ADARQUAH, who was listed as the mother of E.H. The same name is listed as the mother of OFORI in OFORI'S alien file. Ultimately, the passport was issued on May 21, 2012, in the name of E.H., but with a picture of a person who I believe is OFORI. The address listed on the passport application is 249 Ridgeview Drive, Winston Salem, NC 271007. This address was found on a piece of paper found in OFORI'S possession at the time of his recent arrest at the U.S.-Canada border. According to commercial database records, this address is associated with B.C. who is listed on OFORI'S emergency contact information obtained from

Eagle Protection Services and the Prince William County Government. B.C. is listed as OFORI'S sister on the Eagle Protection Service emergency contact form.

14. I have conducted reviews of DHS crossing records for the related passport. The review revealed the passport has been used multiple times to enter the United States. A recent crossing occurred on February 25, 2017 at Dulles International Airport. The passenger's flight originated in Kotoka International Airport in Accra, Ghana.

15. On May 27, 2018, OFORI, traveling with his wife and two children in a rental vehicle, presented himself as E.H. in the inbound vehicle lane from Canada at the Alexandria Bay Port of Entry in New York. OFORI presented a U.S. passport, which bears the name E.H. This passport contains a Ghanaian Immigration Service stamp dated February 24, 2017. During the encounter at primary inspection, CBP Officers conducted various database searches. CBP Officers determined that there was an outstanding arrest warrant for E.H. for failure to appear on grand larceny charges in Virginia. OFORI was then referred to secondary inspection. In secondary inspection, a database showed that OFORI was believed to be using the identification of E.H. and that OFORI was the subject of an HSI criminal investigation. Ultimately, the CBP Officers administratively arrested and detained OFORI based on his outstanding warrant of removal pursuant to U. S. immigration law. OFORI was not arrested under the warrant for E.H., as he is not actually the person wanted in that state matter, but rather is using the identity of E.H.

16. Pursuant to a Customs border search, CBP Officers searched OFORI and his vehicle. A backpack containing the SUBJECT COMPUTER and men's clothing was recovered from the vehicle and searched at the border. OFORI told the CBP Officer that the backpack and the SUBJECT COMPUTER belonged to him. A CBP Officer opened the SUBJECT COMPUTER and saw a log-on screen with OFORI's name. OFORI refused to provide the

password to the SUBJECT COMPUTER.[3] The CBP Officers also found multiple documents folded in OFORI's wallet. OFORI possessed a printout of an email message. The message contained an itinerary from South African Airway for E.H. The itinerary reflected E.H. leaving the United States from Dulles International Airport on February 16, 2017 and traveling to Ghana and returning to the United States at Dulles International Airport on February 24, 2017.[4] The itinerary is dated January 13, 2017.

17. OFORI also had a small piece of paper, which had the biographical information of E.H. on it. This information included E.H's full name, date of birth, time of birth, city of birth, county of birth, father's name, mother's name and mother's place of birth. Based on my experience with identity fraud cases, I believe that this document was created as an aid to OFORI in case he needed to quickly recall this information in furtherance of his identity fraud scheme of E.H.

18. Based on my review of travel databases, I learned that a reservation existed for E.H. to leave the United States. E.H., which was likely OFORI, was scheduled to leave the United States at John F. Kennedy and arrive at Gatwick Airport in London, England on May 29, 2018. Additional reservation information indicates that E.H. was scheduled to return to the United States on June 4, 2018.

FRAUD AND MONEY LAUNDERING SCHEMES

---

[3] At a later date, CBP transferred the SUBJECT COMPUTER to HSI custody in Syracuse, New York. I understand that the SUBJECT COMPUTER has been maintained in such a way that its contents should be preserved in substantially the same way they existed at the time the SUBJECT COMPUTER was first seized by law enforcement.

[4] The itinerary doesn't specifically state the year, only the month and day, but 2017 can be inferred by the overall date of the itinerary.

19. The investigation has revealed that OFORI and other Ghanaian citizen co-conspirators residing in Northern Virginia and elsewhere have engaged in laundering the proceeds of Romance Fraud and BEC fraud.

20. In Romance Fraud, perpetrators search online dating and social media sites in an effort to locate emotionally vulnerable victims - predominantly older, widowed, or divorced women. Once contact is established, the scammer makes every effort to quickly endear themselves to the victim romantically, and frequently even proposes marriage. They make plans to meet in person, but that never actually happens. Eventually, the perpetrator pressures the victim to send them large amounts of money under false pretenses such as urgent medical emergency, unexpected legal fees, or to secure a lucrative overseas contract. If the victim is willing to send funds initially, the perpetrator will come back repeatedly with various false emergencies and business proposals until all of the victim's funds have been exhausted.

21. In a BEC, perpetrators "hack" or gain access to the e-mail accounts of a company or individual. Once they have established access to the e-mail, the perpetrator begins communicating directly with the victim by either using an e-mail address which is very similar to one already known to the victim, or by using a "spoofed" e-mail address which appears on the to from line to be identical to one known to the victim, but is actually concealing the perpetrator's true e-mail address. Often, only an examination of the full e-mail header data will allow for the identification of the real e-mail address. Once communication is established, the perpetrator deceives the individual or company into making payments via wire transfer to bank accounts controlled by the perpetrator. Soon after the wire transfer is completed, the proceeds are withdrawn from the bank account and the funds are laundered.

22. Based upon my knowledge, training, and experience, participation and other information I have learned from other agents who have participated in other investigations involving wire fraud and money laundering, I know that persons participating in these frauds often keep records of their activities to ensure they receive the appropriate payment for their participation. These records may be in written or electronic form. They may consist of spreadsheets, records, receipts, notes, ledgers, money orders, bank records, safety deposit box information, photographs, email addresses, on-line identities, telephone numbers, and other documentation relating to the fraud and subsequent money laundering. This documentary evidence may also include credit card and hotel receipts, plane and other transportation tickets and receipts, car rental receipts, accounts and records in fictitious names, false identification, cashier's checks, and records indicating the existence of storage facilities. These items may be maintained and retained for long periods of time on electronic storage devices, including computers or data storage devices.

23. OFORI and others have used bank accounts in Northern Virginia, and elsewhere, to receive fraudulent wire transfers from individuals and businesses victimized by Romance Fraud and BECs.

24. In furtherance of the investigation, I learned that OFORI has created multiple corporations with the Virginia Corporation Commission. These corporations include Edgar Financial Services, LLC, and Lois Global Associates, LLC. OFORI is the registered agent for these corporations. Using these entities, OFORI opened business bank accounts at Wells Fargo, BB&T Bank, M&T Bank, TD Bank.

Victim 1

25. At various times, I interacted with officials with the OnPoint Community Credit Union, located in the Portland, Oregon area. I learned from these interactions that one of their customers was suspected of being the victim of an elder fraud scheme. The suspected victim (referred herein as C.L.) is approximately eighty-one years old. The credit union came to this belief after C.L. told bank official that she had been befriended on Facebook by a person claiming to be "Sgt. Dave Scott." C.L. had never met "Sgt. Dave Scott" in person. Scott told C.L. that he had a shipment of valuables, which he was trying to send back to the United States, but he needed her to pay for the shipping and customs duties.

26. I was able to obtain banking and wire documentation surrounding these payments. From August 11, 2017 through September 26, 2017, C.L. wired three payments to TD Bank account ending in 8855 and Citi Bank account ending in 7048 for Freeman Auto, LLC. as the beneficiary, which totaled approximately $25,550. On November 6, 2017, C.L. attempted to wire a payment of approximately $92,500 to PNC Bank account ending in 5697 for Ellis Global Services as the beneficiary. This wire documented, "Originator To Beneficiary: For Sgt Dave Scott." OnPoint Credit Union was able to partially stop this transaction and $66,000 was returned to C.L. From December 18, 2017 through December 21, 2017, C.L. sent two wires to Wells Fargo Bank accounts ending in 4265 for Edgar Financial Services LLC as the beneficiary. These wires totaled $61,000. On February 9, 2018, C.L. attempted to wire a $38,500 payment to SunTrust bank account ending in 0264 for Lois Global Associates LLC as the beneficiary. Virginia Corporation Commission identifies OFORI is the registered agent for both Edgar Financial Services LLC and Lois Global LLC.

Victim 2

27. In May 2018, I spoke to a Bank of Ripley bank official in Ripley, Tennessee who informed me that they suspected one of their customer was the victim of an elder fraud scheme. The suspected victim (referred herein as J.S.) is approximately sixty-eight years old and a widow who resides on her family farm in Tennessee. The bank suspected that she was a victim based on her statements about the purpose of her wires and the facts surrounding the recipients of the wire. J.S. informed bank officials that she was sending the wires to help her late husband's friend who was retiring from the military. The friend claimed that he needed to have customs fees paid so that his investments could be release.

28. In January and February 2018, J.S. sent three wires to a Bank of America account ending in 7886. The beneficiary of the wires is listed as Freeman Auto, LLC in East Orange, NJ. These wires totaled approximately $29,660. On February 22, 2018, J.S. wired approximately $71,689.50 to a M&T Trust Bank account ending in 3634. The beneficiary of the wire is listed as Lois Global LLC, 1960 Gallows Road, Vienna, VA. This address appears to be the address for the M&T Trust Bank branch receiving the wire. On April 9, 2018, J.S. wired approximately $97,230.02 to a BB&T account ending in 6048. The beneficiary of the wire is listed as Lois Global LLC, 401 Jefferson Davis Highway, Fredericksburg, Virginia. This location appears to be the address of the BB&T Bank branch receiving the wire. In March, 2018, J.S. wired approximately $67,730.40 to a TD Bank account ending in 9111. The beneficiary of the account is Unilever Global, LLC, 308 Maple Avenue, East Vienna, Virginia. This address is an address for a TD Bank. According to Virginia Corporation Commission records, R.K. is the registered agent of Unilever Global, LLC. I believe R.K. is an assumed identity of OFORI. Facts supporting this suspicion will be documented later in this affidavit. On or about April 23, 2018, J.S. initially attempted to send but recalled a wire a BB&T Bank account ending in 5892. The

beneficiary of the account is Prince Peace Cleaning, 2534 District Ave, Fairfax, Virginia 22030. This wire was for approximately $108,250.

29. In addition to the statements given by J.S. to the Bank of Ripley, the bank also reviewed other evidence surrounding the wires. The bank discovered that Unilever Global LLC., Lois Global LLC. and a third LLC., Pascal Consultancy LLC. were all formed between December 2017 and March 2018. All three corporations were located at the same address Fredericksburg, Virginia, which is a small townhouse style residence. The bank conducted a google internet search of the address and was able to see a street side view of the location. Virginia Corporation Commission records also reflect R.K. is the registered agent of Pascal Consultancy.

30. On May 2, 2018, United States Postal Inspection Service Inspector David Frederick and I spoke with a Fredericksburg, Virginia Police Detective (the Detective) after he learned that there was a federal investigation on OFORI. The Detective indicated that OFORI had assumed the identity of a person identified here by the initials R.K. and was attempting to access a BB&T bank account under that name. The Detective and I interviewed the bank official about the incident on May 3, 2018. The BB&T bank official stated that OFORI, using his true identity, opened a business bank account with BB&T bank on or about February 28, 2018. The name of his business is Lois Global LLC. On or about April 23, 2018, the BB&T bank official called and left a message asking OFORI come in and sign a required form.

31. On or about April 24, 2018, OFORI appeared at the BB&T bank branch in Fredericksburg, Virginia. Believing OFORI was there to sign the form associated with his Lois Global LLC account, the bank official approached OFORI. OFORI indicated that he was having a problem with his account and wanted help with it. The bank official requested the account

information, which OFORI provided. The account information showed that it was a business account for "Pascal Consultancy" with R.K. is its agent. That account had been blocked by BB&T corporate offices after Wells Fargo bank requested that a $77,000 wire to this account be reversed.

32. The BB&T bank official asked OFORI for identification. OFORI initially stated that he did not have identification, but then produced a Ghanaian passport. The passport had a visa in it. The bank official stated that she has many customers who use passports and visas to open and maintain their accounts. The bank official indicated that the visa in the passport was not consistent with others that she has reviewed. She specifically noted the print quality was poor and the picture seemed too big. She indicated that the name on the passport was R.K., which surprised her because she remembered OFORI from opening the Lois Global LLC account not long before.

33. On May 10, 2018, the BB&T bank official called SA Fulton and stated that OFORI (posing again as R.K.) appeared again to inquire about the block on the Pascal Consultancy account. OFORI, presenting himself as R.K., told the bank official that the $77,000 wire was related to a car deal. OFORI again presented a Ghanaian passport with a U.S. visa as his identification. The bank official copied the visa and provided SA Fulton with the copy. The bank official ended the encounter by indicating that she would continue to try to resolve the problem. She also provided SA Fulton with the license plate number of the vehicle that OFORI was driving. Virginia DMV records indicate that the vehicle is registered in the name of OFORI and E.H.

34. I reviewed the copy of the visa. The U.S. visa is a B1/B2 class and Lincoln series visa. The visa bears the name of R.K., nationality of Ghana, control number

XXXXXXXXXXX322, and passport number XXXXX337. The visa has an issue date of April 23, 2014.

35. I conducted multiple searches of the State Department visa database with the information contained on the visa. The visa control number XXXXXXXXXXX322 is an invalid control number. The passport number XXXXX337 is linked to a visa issued to another Ghanaian citizen who was issued a U.S. visa in 2012. This visa was issued to a person other than OFORI or R.K. A broad search was conducted on non-immigrant visas with the last name of R.K. and nationality as Ghana for search criteria. The search yielded no results. Based on database searches, I believe that the R.K. visa and passport are fraudulent.

Victim 3

36. On May 22, 2018, HSI special agents and a United States Postal Inspection Service (USPIS) agent interviewed another suspected victim (referred hereinafter as "A.J.") regarding the payments made during a romance style scam. A.J. stated she had been in contact via Gmail account chat with an individual known to her as John J Smith. A.J. stated that Smith was a General. A.J. stated Smith had asked her to help him retrieve items that were being held by a company in Germany. A.J. stated Smith asked her to pay fees to a company in order to have the items shipped to the United States. Smith told her the items were various things he had accumulated through traveling the world, as well as personal paperwork. Smith claimed that he was currently in Kabul, Afghanistan and he had traveled to Iran and Germany. Smith claimed he was 68 years of age.

37. A.J. stated she was contacted via Gmail electronic mail by a company that identified itself as Source Financial.[5] A.J. said that in addition to the $26,500 sent to Sackey Settlement Group, she had wired $7,500 to an account at Bank of America on January 2, 2018, that benefitted Edgar Financial Services. She stated this wire was also directed by Source and was a payment for the alleged items that belonged to Smith. Specific information related to these bank accounts is unknown at this point. Copies of emails with Source Financial provided by A.J., indicated there were other requests for funds. In November 2017, Source Financial continued to contact A.J. about providing additional funds. On November 8, 2017, Source provided an account name of Hags Logistics, at PNC bank under account ending in 9522 for A.J. to wire funds. Source requested an additional $5,000 on November 21, 2017. A.J. asked Source Financial if she could make a credit card payment on November 29, 2017, and was informed by Source Financial that she would have to instead purchase two iPhones and mail them to Source Financial.

38. On or about May 25, 2018 and subsequently, I began interacting with an FBI special agent who informed me that he was conducting a Romance Fraud and BEC investigation on Fred AGYEMANG (hereinafter AGYEMANG) and Edward NORMANYO (hereinafter NORMANYO). The FBI's investigation identified a Romance Fraud victim who between July and August, 2017 had sent or deposited approximately $73,600 to accounts with AGYEMANG as the signatory. The victim sent the money to someone she had met on-line who she believed was in the military and who needed money to move back to the United States. The victim believed this would allow the military member to return to the United States so that they could

[5] Emails provided show the user name as Source Security and the email address as sourceservices.tm@gmail.com.

have a life together. During the same time period, AGYEMANG wrote six checks, from the accounts that the victim sent or deposited her money, which totaled $21,700. The checks were written to NORMANYO.

39. The FBI's investigation also identified a married couple who was collectively a victim of a BEC fraud scheme. The couple was attempting to purchase a home. On or about September 25, 2017, the couple was sent a spoofed email, which directed them to wire approximately $207,091 to a SunTrust business account for Sackey Settlement Groups LLC (which is mentioned in the section about Victim 3). On September 26, 2017, a male, ultimately identified as NORMANYO, withdrew $191,000 from the SunTrust account.

40. The FBI investigation lead to the execution of a search warrant at the residence of NORMANYO located at 15374 Gunsmith Terrace, Woodbridge, Virginia 22191. I have reviewed some of the evidence that was seized pursuant to the search warrant. Relevant evidence is clearly linked to OFORI. These items include ledgers and/or notes which notate Pascal (which is linked to R.K.-the assumed identity of OFORI) and the name of a farm in Tennessee that is linked to Victim 2, discussed above. Multiple bank statements were found, which are linked to OFORI and his co-conspirators. These statements include: a Bank of America business account (account # ending in 9469) in the name of Edgar Financial Services, LLC (of which OFORI is the registered agent); a TD Bank business account statement, (account # ending in 9111) in the name of Unilever Global, LLC (which is discussed above in regard to Victim 2); a SunTrust account statement (account # ending in 0264) in the name of Lois Global Associates, LLC (which is discussed above in regard to Victim 1), and a TD Bank statement (account # ending in 0466) also in the name of Lois Global Associates, LLC. Of course, OFORI is the registered agent of Lois Global Associates, LLC. Two passport-sized photographs of

OFORI were also seized pursuant to the search warrant. These appear to me to be exact matches to two passport-sized photographs seized from OFORI when he was arrested in New York. I believe that these photographs were being kept by NORMANYO to produce fraudulent documents for OFORI. This is based on OFORI'S use of a false passport and visa (as mentioned above in regard to Victim 2) and the multiple forged passports found bearing NORMANYO'S picture but assumed or falsified identities.

41. On May 4, 2018, I met with a Diplomatic Security Service (DSS) Special Agent. The DSS Special Agent indicated that she had identified another subject who she believed was also engaged in Romance Fraud schemes, one Leslie TETTEH, who has assumed the identity of P.F. The DSS Special Agent indicated that P.F. created PrinceFos Investments in furtherance of the scheme. Multiple bank documents and notes were found in the FBI's search warrant evidence in the NORMANYO matter, which seemed to be linked to PrinceFos Investments or P.F. Some of the notations and names found seem to be variations on the name PrinceFos and P.F. These various names include simply "FOS" or Prince of Peace Cleaning (which are discussed above in the section concerning Victim 1).

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. Based upon my experience, training, and discussion with other law enforcement personnel dedicated to investigating illegal activities, I am aware that criminal organizations often use laptop computers as a device to target fraud victims through the use of public and private online databases. These databases may indicate the vulnerability and profitability of victims based on age, education levels and income. I am also aware that such organizations will communicate through computers to their victims by posing to be true friends and/or acquaintances who are in financial need while they are actually obtaining money from their

victims through false pretenses. Based upon my experience, training, criminal organizations use computers in the production of false documents such as Social Security cards and U.S. visas.

43. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

44. There is probable cause to believe that things that were once stored on the laptop computer may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, an electronic device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media—in particular, a device's internal hard drives—contain electronic evidence of how a device has

been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

45. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the laptop computer is used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the laptop computer because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment

of USB flash storage devices or other external storage media, and the times the device was in use. Electronic file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain PII or gain unauthorized access to a victim account via the Internet, the individual's

electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

g. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the Warrant I am applying for would permit the examination of the device consistent with the Warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the Warrant.

CONCLUSION

46. I submit that this Affidavit supports probable cause for a search warrant authorizing the search of the SUBJECT COMPUTER, described in Attachment A, to seek the items described in Attachment B.

Jason E. Fulton
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 11th day of June 2018 in Syracuse, New York.

Hon. David E. Peebles
United States Magistrate Judge

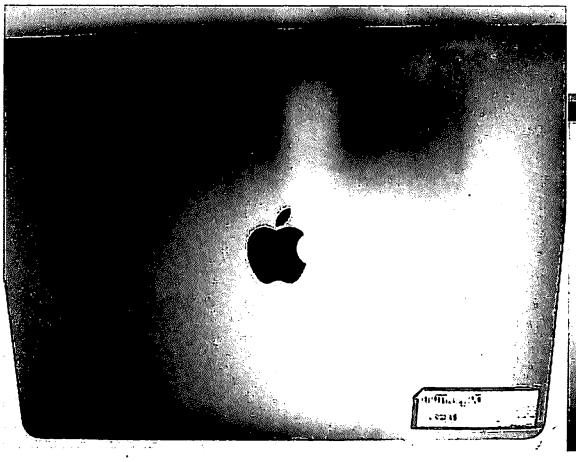
ATTACHMENT A

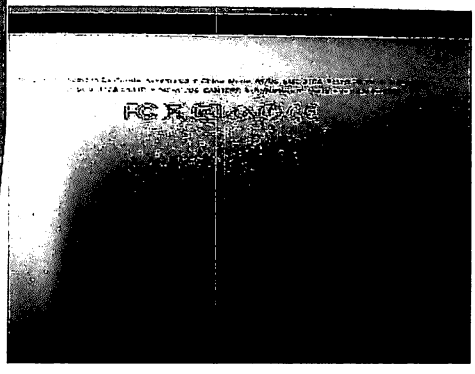
Property to Be Searched

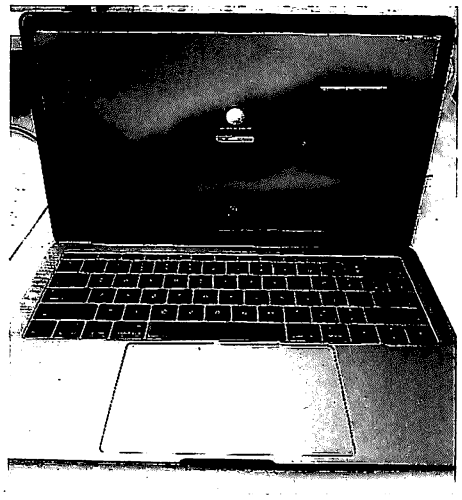
The property to be searched is an Apple Mac Laptop Computer, Model Number: A1708, that is silver in color. The computer is labeled with the serial number: FVFVX2K8Hv22 and FCC ID: BCGA1708.

The Computer currently is located at the Homeland Security Investigations Offices in Syracuse, New York. This Warrant authorizes the forensic examination of the computer for the purpose of identifying the electronically stored information described in Attachment B.

Photographs of the computer to be searched are as follows:







ATTACHMENT B

ITEMS TO BE SEIZED

1. All records on the SUBJECT COMPUTER described in Attachment A that relate to the fruits, instrumentalities and evidence of violations of Title 18, United States Code, Sections 1546 (Visa Fraud),1543 (Passport Fraud), 1544 (Misuse of Passport), 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1030 (Computer Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Wire and Bank Fraud), and 1956(h) (Conspiracy to Launder Monetary Instruments), and involve OFORI and OFORI's co-conspirators, to include:

a. All documents, communications or other information related to the gathering, purchase, theft, sale or use of identities and personal identifying information, including records of Internet activity, such as Internet Protocol ("IP") addresses, browser history, caches, cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

b. All documents, communications or other information related to the use of anonymizer software, including but not limited to The Onion Router ("TOR") browser.

c. All documents, communications or other information related to the transferring or attempted transferring of money by wire, between bank accounts and/or by or between credit card processing accounts, or other means, including the nature, source, destination, and use of those funds.

d. All documents, communications or other information related to the purchase, creation, transmission, or use of stolen, falsified, fraudulent, or fake credit cards, debit cards, gift cards, or other access devices.

e. All documents, communications or other information related to the obtaining, using, selling, or transmitting of stolen, fake, fraudulent, or falsified personal identifying information or financial information, including but not limited to names, Social Security numbers, dates of birth, addresses, credit card numbers, and bank accounts.

f. All documents, communications or other information related to the structuring or other concealment of transfers and/or withdrawals.

g. All documents, communications or other information regarding the usernames, phone numbers, emails, Skype or instant messenger names used by the co-conspirators and/or their associates to transmit information, including personally identifiable information, credit card numbers, and false identification documents used in the schemes.

h. All documents, communications, or other information related to victims of business email compromises, computer intrusions, romance fraud, and related schemes and artifices to defraud victims of money and property that relate to OFORI and his co-conspirators.

i. All documents, communications or other information related to OFORI's or his co-conspirators travel.

j. All business records, bank records, documents and communications related to entities involving OFORI and OFORI's co-conspirators, including: Edgar Financial Services, LLC; Ellis Global Services, LLC; Lois Global Associates, LLC; Freeman Auto, LLC; Unilever Global, LLC; Pascal Consultancy, LLC; Sackey Settlement Group; Hags Logistics; Prince Fos Investments; and Prince of Peace Cleaning.

k. All documents relating to the immigration status, passports, visas and other travel documents associated with OFORI and his co-conspirators.

1. All employment records, employment applications, earnings information, State and Federal tax returns and tax information, and residential information related to OFORI and his co-conspirators.

2. Evidence of user attribution showing who used or owned the at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "documents" "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.